SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT

40 Rector Street, 9th Floor
New York, New York 10006
www.StopSpying.org | (212) 518-7573

MEMORANDUM OF SUPPORT

Date: April 1, 2024
To: All Assembly Members, New York State Assembly; All Senators, New York State Senate; Governor Kathy Hochul
From: The Surveillance Technology Oversight Project (S.T.O.P)

Re: S.T.O.P. Memorandum in Support of Residential Facial Recognition Ban (S.2478 Hoylman-Sigal/A.322 Walker)

S.T.O.P. is a community-based civil rights group that litigates and advocates against discriminatory surveillance. S.T.O.P. works to abolish local governments' systems of mass surveillance. Our work highlights the discriminatory impact of surveillance on Muslim Americans, immigrants, the LGBTQ+ community, indigenous peoples, and communities of color, particularly the unique trauma of anti-Black policing. We craft policies that balance new technologies and age-old rights.

S.T.O.P. emphatically supports the Residential Facial Recognition Ban (A.322/S.2478). This bill would prohibit any landlord from obtaining, retaining, accessing, or using, on any residential premises, any facial recognition system or information obtained from or by the use of such a system. The bill includes a provision establishing Attorney General enforcement and a private right of action for those unlawfully subjected to facial recognition.

Facial recognition has no place in our homes. This technology opens tenants and their guests to harassment and discriminatory eviction or exclusion, and it compromises their privacy. Facial recognition systems discriminate against BIPOC, Muslim, immigrant, and LGBTQ+ New Yorkers. Facial recognition algorithms are up to 100-times more error-prone when attempting to identify young Black women compared to middle-aged white males.[1] Facial recognition also typically assigns each face it scans with one of only two labels—male or female—rendering transgender and non-binary individuals invisible to the algorithm and making them susceptible to misidentification and exclusion.[2]

The racial bias of facial recognition will inevitably impede residents from accessing their homes, locking them out due to mismatches, and may even put them in danger by eliciting an unwarranted law enforcement response. Without legal intervention, collection of biometric data can

[1] Mei Wang and Weihong Deng, *Deep Face Recognition: A Survey*, 215 Neurocomputing 429 (March 14, 2021), https://doi.org/10.1016/j.neucom.2020.10.081; National Institute of Standards and Technology, *NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software* (2019), https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects- race-age-sex-face-recognition-software; Joy Buolamwini and Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 Proceedings in Machine Learning Research 1, Conference on Fairness, Accountability and Transparency (2018), https://dam-prod.media.mit.edu/x/2018/02/06/Gender%20Shades%20Intersectional%20Accuracy%20Disparities.pdf

[2] Rachel Mentz, *AI Software Defines People as Male or Female. That's a Problem*, CNN BUSINESS, Nov. 21, 2019, https://www.cnn.com/2019/11/21/tech/ai-gender-recognition-problem/index.html.

be forced upon not just all residents, but any guests they have over as well, with Black, brown, Asian, and gender non-conforming guests barred from visiting their friends due to facial recognition mismatches.

Landlords will abuse this technology to justify evicting tenants from rent-stabilized units because the facial recognition system determines they were not at home often enough.[3] In fact, vendors have already begun to advertise this technology for such purposes.[4] In public housing, its use has led to residents being evicted for minor violations of policy.[5] One single mother was targeted after she started night classes and asked her ex-husband to spend more time at her home watching their children, causing her to be flagged for potentially violating the housing authority's visitor policy.[6]

Allowing landlords to collect biometric information endangers everyone. In New York City, landlords have been accused of sharing tenants' most sensitive information—phone numbers, photos, and even Social Security numbers—with immigration officials.[7] To protect immigrant communities in our city, we cannot let landlords have access to residents' biometric data. Biometric identifiers are frequently used for access to important public services like ID verification and allocating public benefits.[8] This legislation is necessary to protect residents from hacking and identity theft, as landlords cannot be trusted to implement sufficient protocol to store such sensitive data securely.[9] Unlike other personal identifiers like a social security number, biometric identifiers are static and almost impossible to change.[10] When a hacker acquires another person's biometric data, it puts them at risk for identity theft for the rest of their lives.[11]

Banning biometric surveillance in residences is essential to safeguard New Yorkers from losing their homes or their ability to fully enjoy their rights as tenants. We urge the legislature to pass, and the Governor to sign, the Residential Facial Recognition Ban (A.322/S.2478).

---

[3] *Ask Sam: What Are the Rules for Evicting Rent-Stabilized Tenants in NYC?*, HIMMELSTEIN MCCONNELL GRIBBEN & JOSEPH LLP, Dec. 8, 2021, https://www.brickunderground.com/rent/rules-for-evicting-rent-stabilized-tenant-nyc#:~:text=The%20rent%20stabilization%20code%20requires,she%20can%20begin%20eviction%20proceedings.

[4] Maggie Harrison, *Facial Recognition Used to Evict Single Mother for Taking Night Classes*, FUTURISM, May 17, 2023, https://futurism.com/facial-recognition-housing-projects.

[5] Douglas MacMillan, *Eyes on the Poor: Cameras, Facial Recognition Watch Over Public Housing*, WASH. POST, May 16, 2023, https://www.washingtonpost.com/business/2023/05/16/surveillance-cameras-public-housing.

[6] *Id.*

[7] *See, e.g.*, Lauren Cook, *Queens Landlord Gave Tenant Information to ICE After Discrimination Complaint, Commission Says*, N.Y. DAILY NEWS, July 19, 2017, https://www.amny.com/news/queens-landlord-gave-tenant-information-to-ice-after-discrimination-complaint-commission-says-1.13810387.

[8] *US Government Hack Stole Fingerprints of 5.6 Million Federal Employees*, THE GUARDIAN, Sept. 23, 2015, https://www.theguardian.com/technology/2015/sep/23/us-government-hack-stole-fingerprints. Dan Rafter, *Biometrics and Biometric Data: What Is It and Is It Secure?*, NORTON, May 6, 2022, https://us.norton.com/blog/iot/what-is-biometrics.

[9] A. Dellinger, *Hackers Defeat Vein Authentication by Making a Fake Hand*, ENGADGET, Dec. 28, 2018, https://www.engadget.com/2018-12-28-hackers-defeat-vein-authentication-by-making-a-fake-hand.html.

[10] Anthony Ortega, *Do Biometrics Protect Your Data or Put Your Identity at Risk?*, SPICEWORKS, Oct. 8, 2018, https://www.spiceworks.com/it-security/data-security/articles/do-biometrics-protect-your-data-or-put-your-identity-at-risk/.

[11] *Is Your Identity at Risk from Biometric Data Collection?*, BeyondTrust (last accessed Oct. 6, 2022), https://www.beyondtrust.com/blog/entry/is-your-identity-at-risk-from-biometric-data-collection.